**EXAM OBJECTIVES**

## Exam 70-217

- Install, configure, and troubleshoot the components of Active Directory
  - Implement an organizational unit (OU) structure.
- Manage Active Directory objects.
  - Move Active Directory objects.
  - Publish resources in Active Directory.
  - Locate objects in Active Directory.
  - Control access to Active Directory objects.
  - Delegate administrative control of objects in Active Directory.

CHAPTER

# 8 Administering and Securing Active Directory

Now that you've installed and configured a Windows 2000 computer, it's time to start thinking about managing and securing your resources. In this chapter, you'll learn how to administer and secure Active Directory. To this end, I'll introduce you to Active Directory Users and Computers, a powerful tool you'll use to perform many Active Directory administration tasks. Then I'll show you how to create organizational units (OUs) and configure OU properties. Next, I'll explain how to perform various management tasks with Active Directory objects, including how to locate objects, publish resources, and move objects in Active Directory. Finally, I'll explore how to control access to and delegate administration of Active Directory objects.

## *Chapter Pre-Test*

1. What are OUs, and what is their purpose?
2. List two tasks you can use Active Directory Users and Computers to perform.
3. The act of creating an Active Directory object for a shared folder, shared printer, or other network resource is called _____.
4. Define the terms ***parent object*** and ***child object***.
5. What is the smallest container object in Active Directory to which you can delegate administrative authority?

# Implementing an Organizational Unit (OU) Structure

An *organizational unit* (OU) is a type of Active Directory object. OUs, which are sometimes called container objects, are specifically designed to contain objects and other organizational units from their own domain.

OUs help you organize the structure of Active Directory in much the same way that folders help you organize a file system. You should plan your OU structure before you begin creating OUs. The whole purpose of OUs is to make network administration simpler.

CROSS-REFERENCE

OUs and planning an OU structure were covered in Chapter 2.

In the sections that follow I'll explain how to implement an OU structure, which is accomplished by creating and configuring OUs.

## Creating OUs

Before you can create OUs, you must install Active Directory and create an Active Directory domain that will contain the OUs you create. OUs are created by using Active Directory Users and Computers.

### Active Directory Users and Computers

*Active Directory Users and Computers* is an administrative tool that is a snap-in to the Microsoft Management Console (MMC). You must be an Administrator, a member of the Enterprise Admins group, or a member of the Domain Admins group to have sufficient privileges to use this tool.

In addition to creating OUs, you can use Active Directory Users and Computers to:

- Add users, groups, computers, contacts, printers, and shared folders to Active Directory
- Delete any object in Active Directory

- Configure the properties of any object in Active Directory
- Locate objects in Active Directory
- Publish resources in Active Directory
- Move objects in Active Directory
- Control access to and configure security for Active Directory objects
- Delegate administrative control of Active Directory objects

By default, Active Directory Users and Computers is only installed on domain controllers. However, if you want to create OUs or otherwise administer Active Directory from a nondomain controller (such as your Windows 2000 Professional desktop computer), you can make Active Directory Users and Computers available on any Windows 2000 computer by installing the ADMINPAK. (See the sidebar for more information on installing the ADMINPAK.)

## INSTALLING THE ADMINPAK

The Windows 2000 Administration Tools, called the ADMINPAK, can be installed on any Windows 2000 computer (Professional, Server, or Advanced Server). However, the ADMINPAK files must be installed *from* a Windows 2000 Server or Advanced Server compact disc.

### Installing the ADMINPAK

1. Place the Windows 2000 Server or Advanced Server compact disc in your computer's CD-ROM drive.
2. From the desktop, right-click My Computer, and select Explore from the menu that appears.
3. In the left pane of the My Computer dialog box, click the + next to your CD-ROM drive.
4. Highlight the `I386` folder under your CD-ROM drive. In the right pane of the window, scroll down and double-click the ADMINPAK icon. (The full name of this file is `Adminpak.msi`.)
5. The Windows 2000 Administration Tools Setup Wizard appears. Follow the instructions on-screen to install the ADMINPAK.

To access Active Directory Users and Computers, select Start➪ Programs➪ Administrative Tools➪ Active Directory Users and Computers. Figure 8-1 shows the Active Directory Users and Computers dialog box.

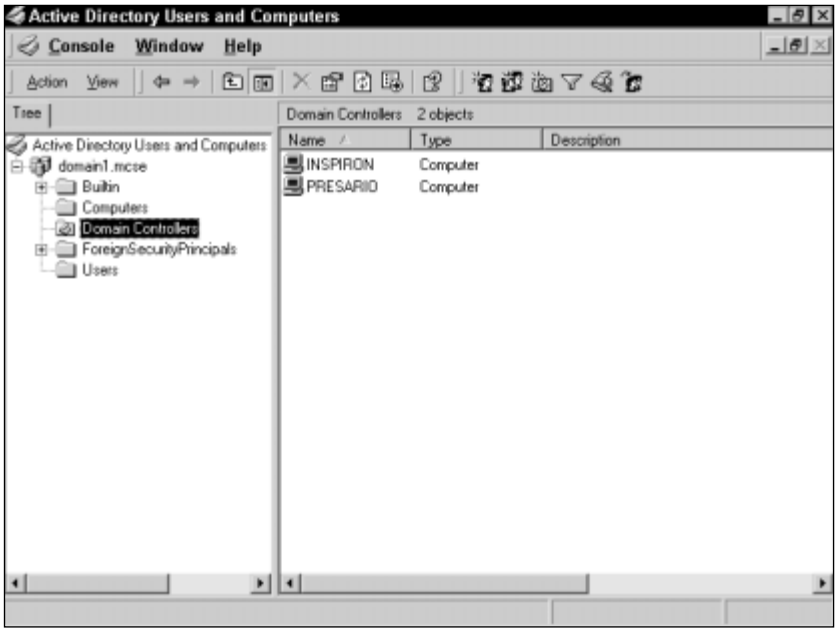


**FIGURE 8-1** Active Directory Users and Computers

Notice the left pane in the dialog box. This pane displays the hierarchical structure of Active Directory in a tree format. Each item displayed in the left pane is an Active Directory object. The Active Directory objects in the left pane are called *container objects* (or sometimes just *containers*) because they can contain other objects. When you highlight an object in the left pane, its contents are displayed in the right pane.

Because you'll probably use Active Directory Users and Computers extensively to create OUs and to manage Active Directory objects, I want to tell you about another way to access this tool.

Microsoft recommends, for security reasons, that you log on as a regular user instead of always as Administrator. However, because you need Administrator privileges to use Active Directory Users and Computers, you'll need to create a shortcut to this tool and configure it to run as Administrator.

STEP BY STEP

### CREATING A SHORTCUT TO ACTIVE DIRECTORY USERS AND COMPUTERS

1. Right-click the desktop, and select New➪Shortcut from the menu that appears.
2. The Create Shortcut wizard begins. In the "Type the location of the item" text box, type **runas /netonly /user:*domain_name*\administrator "mmc.exe dsa.msc"** and click Next.

TIP

Remember to replace italicized text, such as *domain_name*, with your actual domain name, and don't use the underscore—it's just a placeholder.

3. In the "Type a name for this shortcut" text box, type **Active Directory Users and Computers**. Click Finish.
4. The shortcut you just created appears on your desktop. To run Active Directory Users and Computers with Administrator privileges while logged on as regular user, double-click the shortcut on your desktop, and supply the Administrator password when prompted.

## The Process of Creating OUs

Using Active Directory Users and Computers to create OUs is a fairly straightforward process.

STEP BY STEP

### CREATING AN OU

1. Start Active Directory Users and Computers. (Select Start➪Programs➪Administrative Tools➪Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, either highlight the domain in which you want to create an OU, or expand the domain and highlight the OU in which you want to create an OU. Then select Action➪New➪Organizational Unit.
3. In the New Object - Organizational Unit dialog box, type the name you want to assign to the new OU. I recommend that you choose a name that intuitively describes the objects that will be contained in this OU (such as "Accounting Users" for an OU that contains only users who are part of your company's accounting department). Click OK.

STEP BY STEP *Continued*

4. The new OU appears in the right pane of the Active Directory Users and Computers dialog box.

## Configuring OU Properties

After you've created an OU, you may want to configure its properties. Specifically, you can configure a general description of the OU, specify a user account that is responsible for managing the OU, and configure Group Policy for the OU.

STEP BY STEP

### CONFIGURING AN OU

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the domain that contains the OU you want to configure. If the OU you want to configure is displayed in the tree, highlight it.

   If the OU you want to configure is *not* listed in the tree, click the + next to the OU that contains the OU you want to configure. Then, highlight the OU you want to configure.

   Select Action ➪ Properties.
3. The OU's Properties dialog box appears. There are three tabs in this dialog box: General, Managed By, and Group Policy. Configurations on all three of these tabs are optional.

   On the General tab, type any descriptive text you want to enter about the OU. You can enter a general description of the OU and specify a complete geographic address for the OU. Microsoft included this tab because OUs are often based on a physical management location, such as a building, a specific floor of a building, or an office in a specific city. Click the Managed By tab.
4. On the Managed By tab, you can specify the user account that is responsible for managing this OU. To specify a user account, click Change, and select the appropriate user from the list that appears. You can also specify additional contact information about the user you specified if this information is not displayed automatically. To do this, click View, fill in the appropriate information in the user's Properties dialog box, then click OK.

STEP BY STEP *Continued*

5. To configure Group Policy for the OU, click the Group Policy tab and make the necessary configurations. Click OK.

CROSS-REFERENCE

I'll cover Group Policy in great detail in Chapter 10.

Up to this point, you've created an OU and configured its properties. But an OU is really just an empty shell (and of little value) until you create or place objects in it. Some of the objects that you can create or place in an OU include users, groups, computers, printers, contacts, shared folders, and other organizational units. I'll explain how to create these objects in later chapters as I cover the specific topics of users, groups, printers, shared folders, and so on.

# Managing Active Directory Objects

Active Directory objects are generally managed with two primary goals in mind:

- To organize objects in such a way that they are easy for users to locate
- To secure objects and control access to them so that network resources are protected

The primary tool used to manage Active Directory objects is Active Directory Users and Computers.

Some of the most common Active Directory administrative tasks are locating objects in Active Directory, publishing resources in Active Directory, moving objects in Active Directory, controlling access to Active Directory objects, and delegating administration of Active Directory objects. I'll explain how to perform each of these tasks in the sections that follow.

## Locating Objects in Active Directory

One of the benefits of Active Directory is that it's a searchable database. Users can search for (and locate) objects with only a small amount of known information.

For example, suppose I want to send e-mail to a coworker in my company's Denver office, but I only know my coworker's name. I can search Active Directory for all users with that name. When the results of the search are displayed, I can view my coworker's full name, e-mail address, business phone number, and home phone number.

Or, suppose I want to locate a printer in my building that can print in color. I can search Active Directory for all printers with that feature. Then, when the list of results is displayed, I can directly connect to the color printer nearest to me.

There are two tools that users (and administrators) can use to find objects in Active Directory:

- **Active Directory Users and Computers:** This tool is primarily used by administrators, because users normally don't have this tool installed on their computers. If a user has Active Directory Users and Computers installed on his or her computer, he or she can search for an object without having to have Administrator privileges. This tool can be used to search Active Directory for users, contacts, and groups; computers; printers; shared folders; and organizational units.
- **Windows Explorer:** This tool can be used by anyone, and is the only tool that is typically available to all users. This tool can be used to search Active Directory for people, printers, and computers. In addition, you can use Windows Explorer to *browse* Active Directory for shared folders, but you can't use Windows Explorer to search Active Directory for a particular shared folder.

In the next sections I'll show you how to use both of these tools to locate objects in Active Directory.

## STEP BY STEP

### USING ACTIVE DIRECTORY USERS AND COMPUTERS TO LOCATE OBJECTS

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, highlight the domain in which you want to search. Select Action ➪ Find.

STEP BY STEP *Continued*

3. The Find Users, Contacts, and Groups dialog box appears, as shown in Figure 8-2. Notice the "Find" and "In" drop-down list boxes near the top of the dialog box.

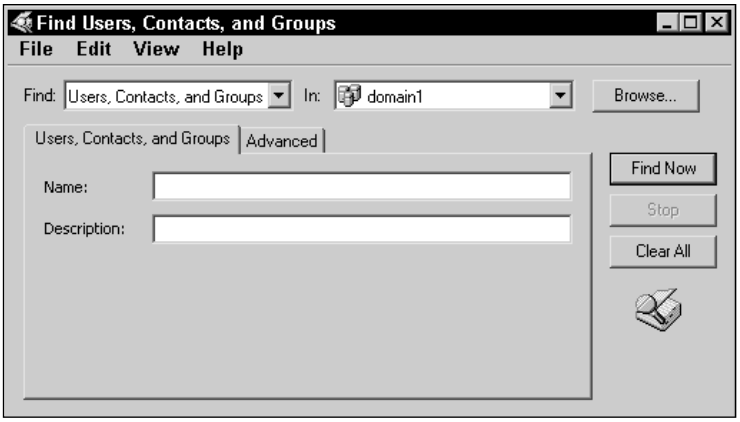


**FIGURE 8-2** Searching for an object in Active Directory

In the "In" drop-down list box, select the domain or OU in which you want to search; or select the Entire Directory, which includes records for all domains in the forest.

In the "Find" drop-down list box, select the type of object you want to locate. The types of objects you can select from are users, contacts, and groups; computers; printers; shared folders; organizational units; or custom search.

Depending on the object you select, a tab specific to that object type is displayed, along with an Advanced tab.

On the object-specific tab, enter any known information about the object you want to locate, as prompted by the tab. Text boxes for information such as the object's name, description, owner, location, model, and so on may be displayed.

Click Find Now to perform the search.

4. Active Directory Users and Computers displays a list of all objects that match the information you specified.

   If the object you searched for is displayed, you can take various actions depending on the type of object. If you searched for a user, contact, or group, you can view and modify the object's properties (if you have the appropriate permissions) by double-clicking the object. If you searched for a printer, you can directly connect to the printer. If you searched for a shared folder, you can map a network drive to that shared folder, and so on.

STEP BY STEP *Continued*

If the object you searched for is not displayed, or if you want to search for multiple objects that all have a similar property, such as all objects located in a particular city, click the Advanced tab and select the specific fields and values you want to search by. Numerous fields are available on this tab—in fact, you can search for an object by virtually any of its properties.

5. Close the Find Users, Contacts, and Groups dialog box.

Windows Explorer is also a useful tool for locating objects in Active Directory. In the steps that follow I'll show you how to search for a person, printer, and computer. I'll also explain how to use Windows Explorer to browse for shared folders.

STEP BY STEP

### STARTING AN ACTIVE DIRECTORY SEARCH IN WINDOWS EXPLORER

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the Windows Explorer dialog box, select View ➪ Explorer Bar ➪ Search, or click the Search button in the toolbar.
3. The Search Explorer bar is displayed in the left pane. The following steps explain how to perform a search for a person, printer, or computer, and how to browse for a shared folder. Continue on to the appropriate set of steps.

### SEARCHING FOR A PERSON

1. To search for a person, in the Search Explorer bar, scroll down and click People.
2. The Find People dialog box appears, as shown in Figure 8-3. Notice the "Look in" drop-down list box.

STEP BY STEP *Continued*

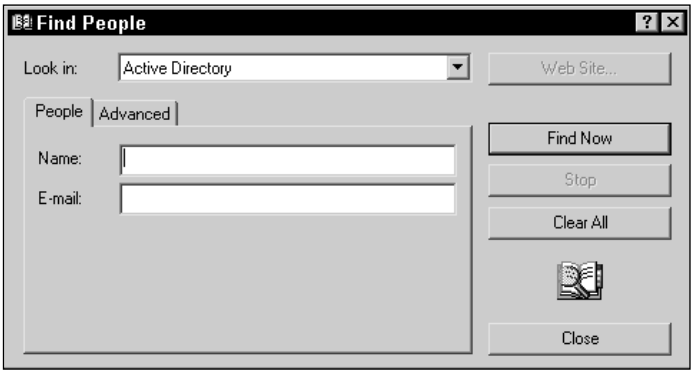


**FIGURE 8-3** Searching for a person in Active Directory

If Active Directory is not selected in the "Look in" drop-down list box, select it.

On the People tab, fill in any known information about the person you want to find, such as the person's first name, last name, or a portion of their e-mail address. Click Find Now to perform the search.

3. Windows Explorer displays a list of all people that match the information you specified.

   If the person you searched for is displayed, you can view the person's full name, e-mail address, business phone number, and home phone number. You can click Properties to view and/or modify detailed information about the user (if you have the appropriate permissions). You can also click Add to Address Book to add this user to your Outlook Express Address Book.

   If the person you searched for is not displayed, you can click the Advanced tab and define advanced search criteria that you want Windows Explorer to search by.

## SEARCHING FOR A PRINTER

1. To search for a printer, in the Search Explorer bar, scroll down and click Printers.
2. The Find Printers dialog box appears. This dialog box has three tabs: Printers, Features, and Advanced.

   In the "In" drop-down list box, either accept the default of Entire Directory, or select a domain you want Windows Explorer to search.

   On the Printers tab, specify any known information about the printer you want to search for, such as its name, location, or model.

   The Features tab is shown in Figure 8-4. Notice that on this tab you can specify which features the printer you're searching for must have.

STEP BY STEP *Continued*

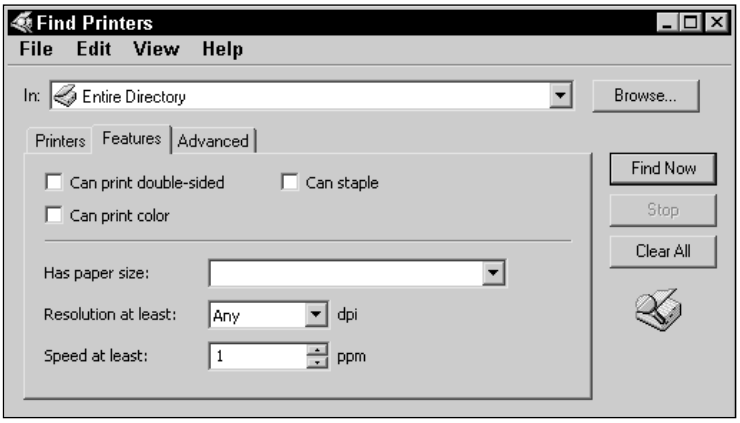


**FIGURE 8-4** Specifying printer features before a search

Also notice that on the Features tab you can select from multiple options, such as double-sided printing, stapling, color printing, and so on. Select the features you need.

On the Advanced tab you can select the specific fields and values you want to search by. Numerous fields are available on this tab—in fact, you can search for a printer by virtually any of its properties.

Once you've made all configurations you want to on the Printers, Features, and/or Advanced tabs, click Find Now to search.

3. Windows Explorer displays a list of all printers that match the information you specified. In addition to the printer's name, the location, model, server the printer is connected to, and comments (if any) are displayed for each printer listed.

   If you want to connect to one of the printers listed, right-click the printer and select Connect from the menu that appears. Windows 2000 will install drivers for that printer on your computer (if not already installed) and will connect to the printer.

   You can also view the printer's properties by right-clicking the printer and selecting Properties from the menu that appears. If you have the appropriate permissions, you can edit the printer's properties, as well.

## SEARCHING FOR A COMPUTER

1. To search for a computer, in the Search Explorer bar, scroll down and click Computers.
2. The Search for Computers screen appears in the Search Explorer bar. In the Computer Name text box, type in any known part of the name of the computer you want to search for. Click Search Now.

STEP BY STEP *Continued*

3. Windows Explorer displays the results of the computer search in the right pane. Figure 8-5 shows both the Search for Computers Explorer bar and the computer search results.

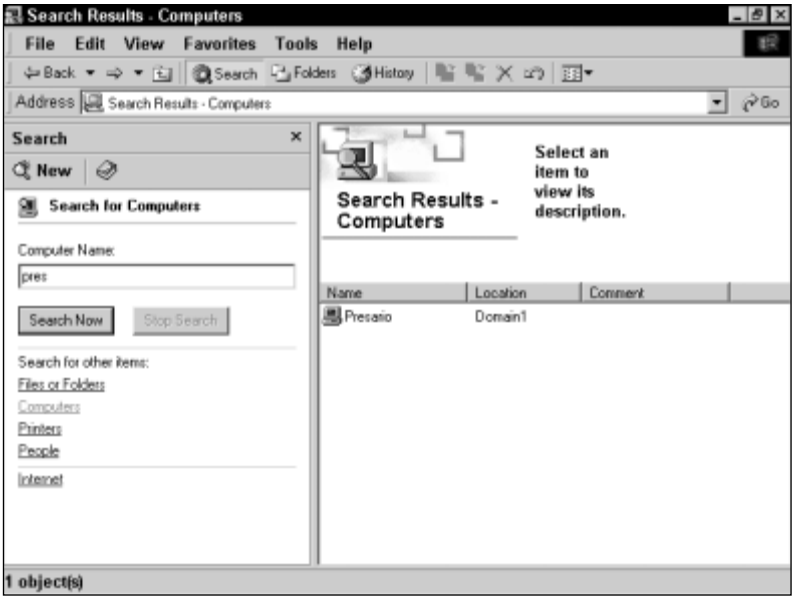


**FIGURE 8-5** Computer search results

All computer names that contain the letter combination you specified in Step 2 are listed in the computer search results. In addition to the computer's name, the location and comments (if any) are displayed for each computer listed.

If you right-click any computer listed in the search results pane, you can select from numerous options in the menu that appears, including:

- **Open Containing Folder:** If you select this option, Windows Explorer opens a dialog box for the domain in which the computer is located. This dialog box lists all computers in this domain. You can open, explore, create a shortcut to, or view the properties of any computer listed.
- **Open:** If you select this option, Windows Explorer graphically displays all of the shared folders, shared printers, the `Scheduled Tasks` folder, and the `Printers` folder for the computer. You can map a network drive to a shared folder; connect to a shared printer; or open, explore, or create a shortcut to any of the folders listed.

STEP BY STEP *Continued*

- **Explore:** If you select this option, a Windows Explorer window is opened that shows the computer's location on the network in the left pane, and a graphical list of the shared folders, shared printers, the `Scheduled Tasks` folder, and the `Printers` folder for the computer. You can browse the network; map a network drive to a shared folder; connect to a shared printer; or open, explore, or create a shortcut to any of the folders listed.
- **Create Shortcut:** If you select this option, Windows 2000 enables you to create a shortcut to this computer on your desktop.
- **Properties:** If you select this option, a few general properties of the computer are displayed.

## BROWSING FOR A SHARED FOLDER

1. To browse for a shared folder in Active Directory, in Windows Explorer, select View ➪ Explorer Bar ➪ Folders.
2. The Folders Explorer bar appears in the left pane. Click the + next to My Network Places. Click the + next to Entire Network. Click the + next to Directory. Click the + next to the domain you want to browse. Beneath the domain, highlight the container object you want to browse.
3. The contents of the container object you selected, including the container's shared folders, shared printers, users, groups, computers, and so on, are displayed in the right pane. Figure 8-6 shows an OU highlighted in the left pane, and the two shared folders it contains displayed in the right pane.

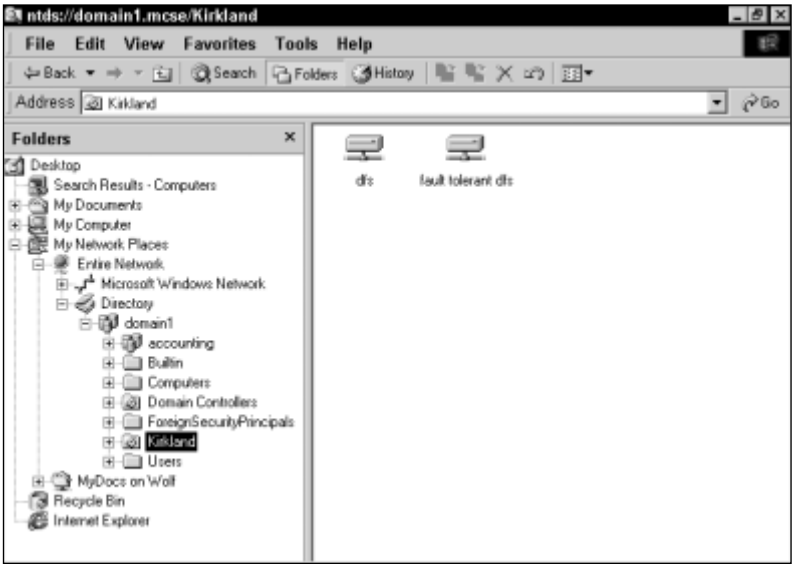


**FIGURE 8-6** Browsing for shared folders

STEP BY STEP *Continued*

If you right-click any of the shared folders displayed, you can open, explore, search, map a network drive to, create a shortcut to, or view the properties of the shared folder.

## Publishing Resources in Active Directory

In order for users and administrators to locate objects in Active Directory, those objects must exist in Active Directory. Windows 2000 automatically creates some objects in Active Directory as the resources they represent are created, but other objects must be manually created in Active Directory by an administrator. The act of creating an Active Directory object for a shared folder, shared printer, or other network resource is called *publishing*.

You don't have to publish shared resources in Active Directory for users to be able to access those resources. For example, users can use Windows Explorer to browse the network to locate a shared printer or a shared folder. However, the advantage of publishing resources in Active Directory is that, because Active Directory is a searchable database, it provides an additional means for users to easily locate these resources.

### Resources That Can Be Published

When you create a user, contact, group, or OU, you are creating an Active Directory object. Because of this, the object for the user, contact, group, or OU is automatically published in Active Directory when you create it. (I explained how to create OUs earlier in this chapter, and I'll show you how to create users and groups in Chapter 9.)

In similar fashion, when a computer joins a Windows 2000 domain, a computer object for the computer joining the domain is created and automatically published in Active Directory. In addition, you can manually publish a computer object in Active Directory for a computer that has not yet joined a Windows 2000 domain.

Shared printers are sometimes automatically published in Active Directory, but this is not always the case. When you create a shared printer on a Windows 2000 computer that is a member of a Windows 2000 domain, Windows 2000 automatically creates a shared printer object and publishes it in Active Directory. However, you must manually publish Active Directory objects for shared printers on Windows NT computers.

Folders, once they have been created and shared on a network server, must always be manually published in Active Directory.

TIP

Publishing a shared folder or printer in Active Directory doesn't create the shared folder or printer. Instead, it creates an object in Active Directory that represents the previously created and shared folder or printer.

Some network services, such as Certificate Services, can be published in Active Directory. These services can't be published manually, but rather are published automatically during installation if their installation programs provide that capability.

## How to Manually Publish Resources in Active Directory

After you have created and shared folders or printers, you can use Active Directory Users and Computers to manually publish objects that represent these resources in Active Directory, as the steps that follow explain.

### STEP BY STEP

#### PUBLISHING SHARED FOLDERS AND SHARED PRINTERS IN ACTIVE DIRECTORY

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, either highlight the domain in which you want to create the shared folder or shared printer; or, expand the domain and highlight the OU in which you want to create the shared folder or shared printer.

   To create a shared folder, select Action ➪ New ➪ Shared Folder.

   To create a shared printer, select Action ➪ New ➪ Printer.
3. If you are creating a shared folder, in the New Object - Shared Folder dialog box, type the name you want to assign to the new shared folder, and enter the full network path to the shared folder. Click OK.

   If you are creating a shared printer, in the New Object - Printer dialog box, type the full network path to the shared printer. Click OK.
4. The new shared folder or shared printer appears in the right pane of the Active Directory Users and Computers dialog box.

## Moving Objects in Active Directory

Occasionally you may need to move objects in Active Directory. Suppose, for example, that an employee is transferred from your company's San Francisco office to your New York office. If your company uses OUs to manage users, groups, and computers by city, you would need to move this employee's user object from the San Francisco OU to the New York OU.

When an OU is moved in Active Directory, all of the OU's contents are moved, as well. Moving an OU in Active Directory is much like moving a folder in a volume.

When an object is moved in Active Directory, several things happen:

- The moved object acquires the inheritable permissions from its new parent object.
- The moved object loses all previously inherited permissions from its old parent object.
- Any previously explicitly assigned permissions to users and groups for this object are retained. In other words, the same users and groups that could access or manage this object before it was moved can access the object after it is moved, if their permissions were explicitly assigned, and not inherited.

The new parent object is the domain, OU, or other container object in which the moved object is placed. I'll define and discuss permissions in greater detail a little later in this chapter.

EXAM TIP

Make sure you understand what happens to an Active Directory object's permissions when the object is moved. Since the process of moving an object is pretty simple, expect the exam to focus more on permissions than on the moving process.

### Moving Objects within a Domain

You can use Active Directory Users and Computers to move an object within a domain, as the steps that follow explain.

## STEP BY STEP

### MOVING AN OBJECT IN ACTIVE DIRECTORY

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the object you want to move. Highlight the OU or other container object that contains the object you want to move.

   In the right pane, right-click the object you want to move, and select Move from the menu that appears.
3. The Move dialog box appears, as shown in Figure 8-7. Notice that a list of all container objects in the domain is displayed.

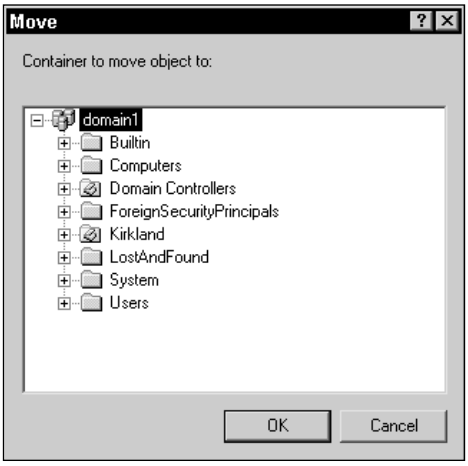


**FIGURE 8-7** Moving an object in Active Directory

   Expand the OUs or other container objects in this dialog box as necessary. Highlight the OU or other container object in which you want to place the object you are moving. Click OK.
4. Windows 2000 moves the object, and returns you to the Active Directory Users and Computers dialog box.

### Moving Objects to a Different Domain

If you need to move an object to a different domain, you won't be able to use Active Directory Users and Computers to get the job done. You can use the `MoveTree.exe` command-line utility to move objects from one domain to another. `MoveTree.exe` is not installed by default. You can make `MoveTree.exe` available by installing the Windows 2000 Support Tools, which are located on the Windows 2000 Server/Advanced Server compact disc in the `\Support\Tools` folder.

For more information on using `MoveTree.exe`, install the Windows 2000 Support Tools, then select Start ➪ Programs ➪ Windows 2000 Support Tools ➪ Tools Help, and search for MoveTree.

## Controlling Access to Active Directory Objects

Access to Active Directory objects can be controlled by assigning Active Directory permissions to users, groups, and computers that may attempt to access these objects. It's normally a good practice to control access to Active Directory objects in order to prevent undesired modification (either intentionally or unintentionally) of the objects, and to enable specific users and groups to administer objects in Active Directory.

Controlling access to an object in Active Directory is *not* necessarily the same as controlling access to the object itself. When a component (such as a computer, shared folder, or shared printer) exists outside of Active Directory, and also has a corresponding object in Active Directory, the permissions set on the Active Directory object do not affect the permissions to the actual component itself.

For example, suppose I have permission to write to a shared folder on my network. That doesn't necessarily mean I have permission to write to the object that represents this shared folder in Active Directory. Or, suppose I have Full Control over a shared printer object in Active Directory. I may or may not have permissions to print to this printer, depending on how the administrator has configured the printer's permissions.

TIP

Active Directory permissions only specify whether a user, group, or computer can view or modify an object's properties in Active Directory. Active Directory permissions do *not* control access to the shared folders or shared printers themselves.

In the real world you may not have to modify the security properties on Active Directory objects, because the default security permissions of the Windows 2000 built-in groups are often adequate for small to medium-sized organizations. Once an administrator makes users members of appropriate groups, the users have permissions to Active Directory objects suitable for the users' job tasks and responsibilities.

EXAM TIP

Even if you don't have to set permissions on Active Directory objects on your company's Windows 2000 network, make sure you understand and know how to apply these permissions before you take the Directory Services exam.

## Permissions Terminology

Before I move on to the process of setting permissions on Active Directory objects, there are a few terms I need to define, which are used throughout the Windows 2000 user interface. Two of these terms are *parent object* and *child object*. A parent object is a container object that contains other objects. An object that is contained in the parent object is referred to as a child object.

Another important term is *inheritance*. Inheritance refers to the permissions an object receives simply because it is contained in another object — in other words, because an object is a child (or grandchild) object of a particular parent object. When an object inherits permissions, it's not because the permissions have been applied specifically to the object in question, but rather because permissions have been set on the parent object that contains the object in question. An important feature of inheritance is that when permissions are configured to apply to all of an object's child objects, the permissions are applied to *all* objects contained in the parent object's tree, regardless of how many intermediate containers exist between the child object and the parent object to which the permissions have been assigned.

## Setting Permissions on Active Directory Objects

You can use Active Directory Users and Computers to set permissions on Active Directory objects. This tool provides you with a great deal of control when it comes to assigning permissions to objects.

Permissions are set in Active Directory Users and Computers by modifying the security properties of an Active Directory object. When you configure the permissions of an Active Directory object, you can:

- Specify the users and groups that are specifically permitted or denied access to the object or its properties
- Specify whether the object's permissions will be applied to only the object itself, or to the object and to all of its child objects
- Specify whether the object will inherit permissions from its parent object. (If you configure an object to *not* inherit permissions from its parent object, this is referred to as *blocking inheritance*.)
- Configure permissions to control access to a specific property of the object

There are numerous permissions that can be set for Active Directory objects. The specific permissions that can be set for each object vary, depending on the type of object. That said, there are five standard Active Directory permissions that can be applied to most objects in Active Directory. Table 8-1 lists and describes each of these permissions.

**TABLE 8-1 Standard Active Directory Permissions**

| Permission | Description |
|---|---|
| Full Control | Assigns *all* permissions to the specified user or group for this object, including permission to: delete the object; delete the subtree; view or edit the object's properties, including permissions; take ownership of the object; configure auditing for the object, and so on. |
| Read | Permits the specified user or group for this object to list the contents of the object; and read all of the properties of this object, including its permissions. |
| Write | Permits the specified user or group for this object to write all properties of this object. However, the write permission does *not* permit the specified user or group to take ownership of the object, modify permissions, or configure auditing. |
| Create All Child Objects | Permits the specified user or group for this object to create all child objects for this object, including computer objects, contact objects, group objects, organizational unit objects, printer objects and so on. |
| Delete All Child Objects | Permits the specified user or group for this object to delete all child objects for this object, including computer objects, contact objects, group objects, organizational unit objects, printer objects and so on. |

In addition to standard permissions, there are numerous advanced permissions that can be set on Active Directory objects. These advanced permissions enable precise, granular access control to Active Directory objects.

TIP

I recommend, for ease of administration, that you assign permissions to groups instead of users whenever possible. I also recommend that you assign permissions as high in the domain tree as possible and rely on inheritance to propagate permissions down the tree.

Now I'll explain the steps involved in assigning permissions to Active Directory objects.

## STEP BY STEP

### CONFIGURING PERMISSIONS ON ACTIVE DIRECTORY OBJECTS

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the Active Directory Users and Computers dialog box, select View ➪ Advanced Features. (You must select this option before the Security tab will become available.)
3. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the object for which you want to configure permissions. In the left pane, continue expanding the domain tree until the object you want to set permissions on is displayed. Then right-click the object, and select Properties from the menu that appears.
4. In the object's Properties dialog box, click the Security tab.
5. The Security tab is displayed. Figure 8-8 shows the Security tab for an OU named Kirkland. Notice that various users and groups are displayed in the top section of this tab. Only users or groups that have some sort of permission to view or modify one or more properties of this object are listed. Also notice that permissions for the highlighted user or group are listed in the bottom section of this tab.

   First, highlight the user or group to which you want to assign permissions. (If the user or group you want to assign permissions to is not listed in this dialog box, click Add. Then, in the Select Users, Computers, or Groups dialog box, double-click the user or group you want to add, and click OK.)

   Then, in the permissions box, select the permission(s) you want to allow or deny to the user or group you selected by selecting the appropriate "Allow" or "Deny" check box(es).

STEP BY STEP *Continued*

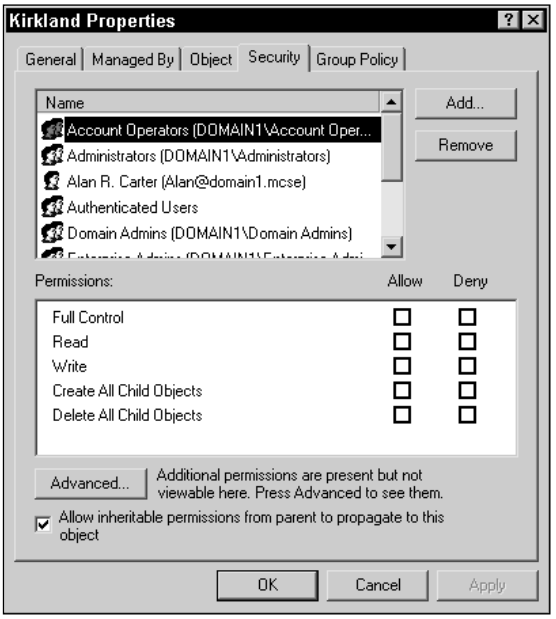


**FIGURE 8-8** The Security tab

If you want to block inheritance to this object, clear the check box next to "Allow inheritable permissions from parent to propagate to this object." This check box is selected by default.

If you want to configure advanced permissions, or if you want the permissions you assign to be inheritable by child objects of this object, click Advanced. (If you are done configuring permissions, skip to Step 9.)

6. The Access Control Settings dialog box for the object is displayed. Figure 8-9 shows the Access Control Settings dialog box for an OU. Notice the detailed permission entries listed.

   To configure advanced permissions, highlight the user or group (listed in the Name column) for which you want to edit permissions. Then click View/Edit.

7. The Permission Entry dialog box for the object appears. Figure 8-10 shows the Permission Entry for Kirkland dialog box. Notice that the user or group you selected in Step 6 appears in the Name list box. Also notice the detailed list of permissions and the "Apply onto" drop-down list box.

STEP BY STEP *Continued*

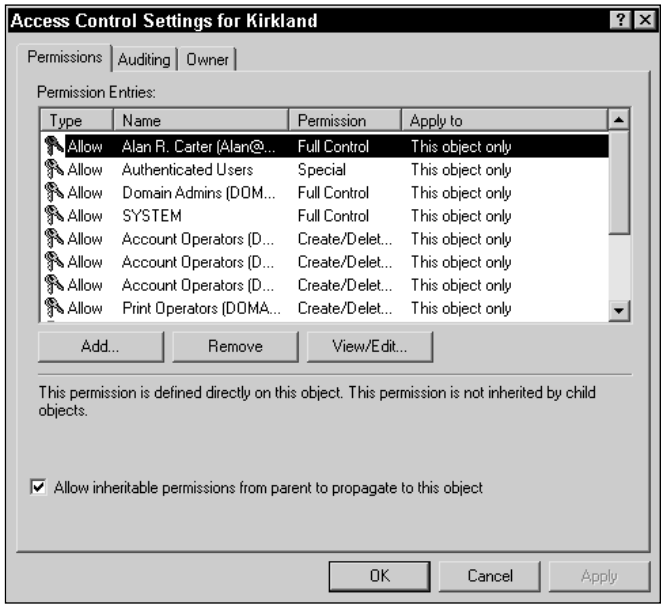


**FIGURE 8-9** Access control settings

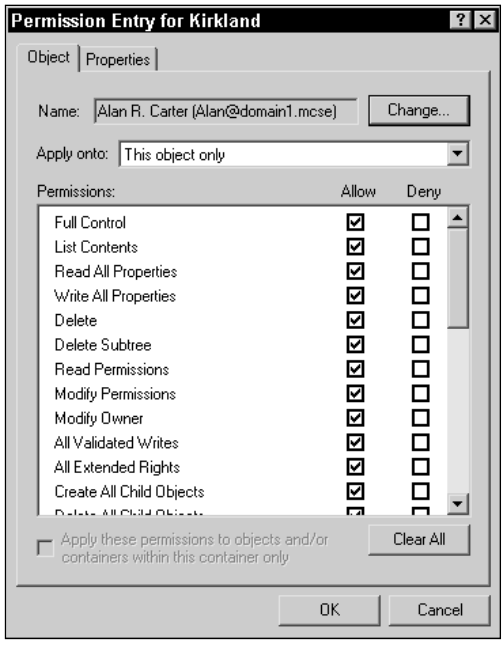


**FIGURE 8-10** Configuring advanced permissions

STEP BY STEP *Continued*

By default, the permissions you configure will apply to *this object only*. However, if you want to use inheritance to propagate this permission to child objects, select the "This object and all child objects" option from the "Apply onto" drop-down list box.

TIP

You must manually change the setting in the "Apply onto" drop-down list box if you want to use inheritance to propagate the permissions you're configuring.

In the Permissions box, select or clear the check boxes next to the permissions you want to modify for the selected user or group. Click OK.

8. The Access Control Settings dialog box for the object reappears. Click OK.
9. In the object's Properties dialog box, click OK.

## Taking Ownership of an Active Directory Object

Occasionally, you may need to assign permissions to an Active Directory object, but not have the Full Control permission for the object. Without the Full Control permission (or the Modify Permissions specific permission), you can't assign or change an object's permissions. This situation can arise if an administrator accidentally changes his or her own permissions so that he or she no longer has the Modify Permissions permission, or if a delegated administrator removes a senior administrator's permissions to the object.

To remedy this situation, you must take ownership of the Active Directory object. The owner of an object can always assign permissions to that object.

You can take ownership of an Active Directory object if you are a member of the Domain Admins group or have the Modify Owner permission to the object.

The steps that follow explain how to take ownership of an Active Directory object.

STEP BY STEP

TAKING OWNERSHIP OF AN OBJECT IN ACTIVE DIRECTORY

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the Active Directory Users and Computers dialog box, select View ➪ Advanced Features.
3. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the object for which you want to take ownership. In the left pane, continue expanding the domain tree until the object you want to take ownership of is displayed. Then right-click the object, and select Properties from the menu that appears.
4. In the object's Properties dialog box, click the Security tab.
5. On the Security tab, click Advanced.
6. In the Access Control Settings for the object dialog box, click the Owner tab.
7. The Owner tab appears. In the "Change owner to" box, highlight your user name (or group). Click OK.
8. In the object's Properties dialog box, you can now assign permissions to this object as desired. Click OK.

## How Active Directory Permissions Combine

It is not uncommon for a user to have permissions to an Active Directory object and to be a member of one or more groups that also have permissions to that object. These permissions may either be assigned directly to the object, or may be inherited from a parent object.

When user and group permissions to an Active Directory object differ, the user and group permissions are additive, and the *least* restrictive permission is the user's effective permission. For example, a user has the Read permission to an Active Directory object, and a group that the user is a member of has the Full Control permission to the object. The user's effective permission to the object is Full Control.

However, there is an exception to this rule. First, if the user, or any group the user is a member of, is *denied* a specific permission, then the user is denied that permission. For example if a user is allowed the read permission, and a group the user is a member of is denied the read permission, then the user is denied the read permission. When an allow permission and a deny permission combine, the deny permission takes precedence. I like to

call this exception "the deny rule." The Full Control permission can be particularly troublesome here. If the user (or any group that the user is a member of) is denied the Full Control permission, the user is denied *all permissions* to the Active Directory object. For this reason, you should use great care when denying a permission to a user or group.

However, even the deny rule has an exception. If a specific user (or group) is denied a permission at the parent object level, and that user (or group) is directly allowed that permission (or a permission that includes that permission) at the object level, then the directly assigned permission (called an *explicit permission*) takes precedence, and even overrides the denied permission. For example, suppose a user is denied the Write permission to an OU, and is also assigned the Full Control permission to a child object of the OU. At the child object level, then, the user is denied the Write permission by inheritance, but is explicitly assigned the Full Control permission. The user's effective permission to the child object is Full Control, because this permission was explicitly assigned at the child object level.

## Delegating Administration of Active Directory Objects

Delegation is one of the many benefits of Active Directory. Delegation is useful, particularly in large organizations, because it enables the administrator to distribute administrative tasks among several assistant administrators without giving each assistant administrative privileges to the entire network.

Delegation is accomplished by assigning the appropriate permissions to an assistant administrator for a manageable-sized portion of Active Directory, typically an OU. Once this permission is assigned to an assistant administrator for the OU, the assistant can manage the entire OU, including all of its child objects.

The OU is the smallest container object in Active Directory to which you can delegate administrative authority.

There are two primary ways to delegate administration of Active Directory objects:

- You can use Active Directory Users and Computers to manually assign the appropriate permission(s) to the assistant administrator for the Active Directory object, and configure this permission(s) to apply to "This object and all child objects." (To do this, see the step-by-step section titled "Configuring permissions on Active Directory objects" earlier in this chapter.)

TIP

Sometimes administrators want to delegate authority to an assistant for all objects *in* the OU, but not to the actual OU itself. In this case, select the "Child objects only" option instead of the "This object and all child objects" option when configuring advanced permissions.

- You can use the Delegation of Control Wizard in Active Directory Users and Computers. I'll explain how to use this wizard in the next section.

## STEP BY STEP

### USING THE DELEGATION OF CONTROL WIZARD

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the object for which you want to delegate authority. In the left pane, continue expanding the domain tree until the object you want to delegate authority of is displayed. Then right-click the object, and select Delegate Control from the menu that appears.
3. The Delegation of Control Wizard starts. Click Next.
4. In the Users or Groups screen, click Add.
5. In the Select Users, Computers, or Groups dialog box, double-click the user (or group) you want to delegate control to. (If you want to delegate authority to more than one user or group, double-click each one.) Click OK.
6. In the Users or Groups screen, click Next.
7. The Tasks to Delegate screen appears, as shown in Figure 8-11. Notice the various tasks you can delegate.

   If the task(s) you want to delegate to the user or group you selected in Step 5 are listed on this screen, select the task(s). Click Next, and skip to Step 10.

   If the task you want to delegate to the user or group you selected in Step 5 is *not* listed on this screen, select the "Create a custom task to delegate" option, and click Next.

TIP

For purposes of using this wizard only, think of a "custom task" in terms of assigning specific permissions to a specific user for a specific Active Directory object (or for a particular type of child object contained in that object).

STEP BY STEP *Continued*

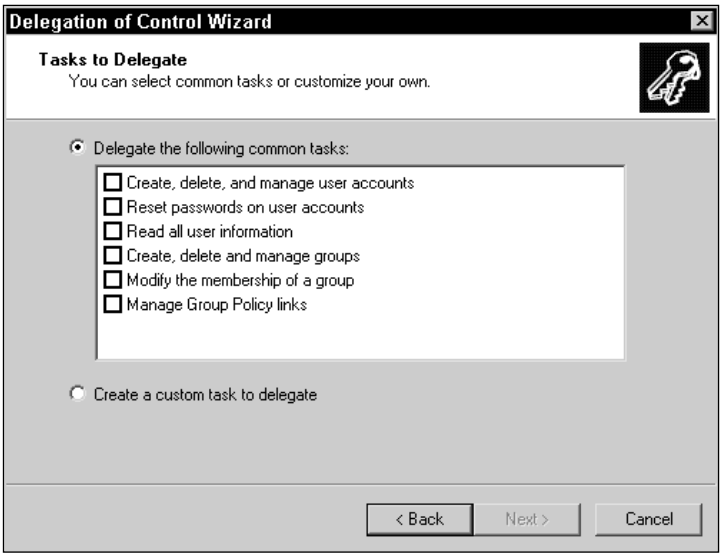


**FIGURE 8-11** Delegating tasks

8. The Active Directory Object Type screen appears. In this screen you specify the scope of the task you want to delegate. You can choose to either delegate control of this entire object, or to delegate control of specific child objects contained in this object. Select the appropriate option and click Next.
9. The Permissions screen appears, as shown in Figure 8-12.

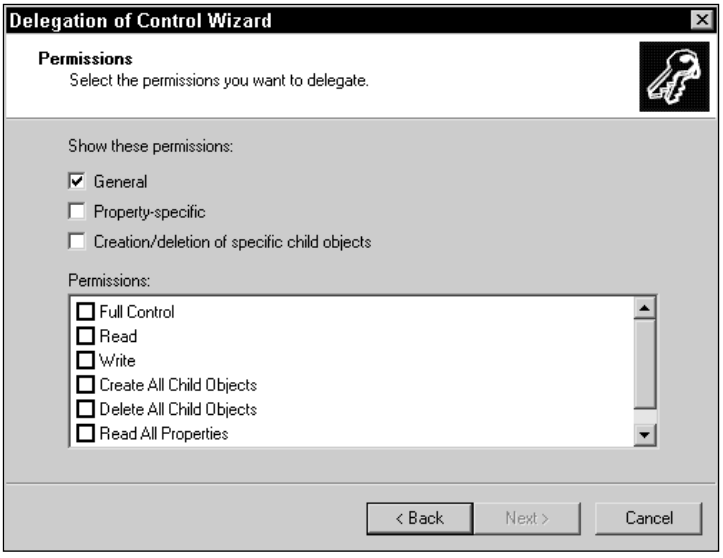


**FIGURE 8-12** Specifying permissions

STEP BY STEP *Continued*

In the top half of this screen, select the type(s) of permissions you want to assign. Then, in the Permissions box, select the specific permissions you want to assign. Click Next.

10. In the Completing the Delegation of Control Wizard screen, click Finish.

## KEY POINT SUMMARY

This chapter introduced several important Active Directory topics:

- An organizational unit (OU) is a type of Active Directory object. The whole purpose of OUs is to organize users, computers, and other Active directory objects to simplify network administration .
- Active Directory Users and Computers is the primary administrative tool used to perform management tasks with OUs and other Active Directory objects. By default, this tool is only installed on domain controllers, but you can make it available on any Windows 2000 computer by installing the ADMINPAK.
- There are two tools that users (and administrators) can use to find objects in Active Directory: Active Directory Users and Computers and Windows Explorer.
- The act of creating an Active Directory object for a shared folder, shared printer, or other network resource is called publishing. The advantage of publishing resources in Active Directory is that, because Active Directory is a searchable database, it provides an additional means for users to easily locate these resources.
- Windows 2000 automatically publishes some objects in Active Directory as the resources they represent are created, but other objects must be manually published in Active Directory by an administrator.
- You can use Active Directory Users and Computers to move an object within a domain. The `MoveTree.exe` command-line utility is used to move objects from one domain to another.

- When an OU is moved in Active Directory, all of the OU's contents are moved, as well.
- A parent object is a container object that contains other objects. An object that is contained in the parent object is referred to as a child object.
- Access to Active Directory objects can be controlled by assigning Active Directory permissions to users, groups, and computers that may attempt to access these objects. Permissions are set by modifying the security properties of an Active Directory object.
- When you configure the permissions of an Active Directory object, you can:
  - Specify the users and groups that are specifically permitted or denied access to the object and/or its properties
  - Specify whether the object's permissions will be applied to only the object itself, or to the object and to all of its child objects
  - Specify whether the object will inherit permissions from its parent object
  - Configure permissions to control access to a specific property of the object
- Occasionally, you may need to assign permissions to an Active Directory object, but not have the Full Control (or the Modify Permissions) permission for the object. To remedy this situation, an Administrator must take ownership of the object.
- It's not uncommon for a user to have permissions to an Active Directory object and to be a member of one or more groups that also have permissions to that object. In general, user and group permissions are additive, and the *least* restrictive permission is the user's effective permission. But there are exceptions.
- Delegation is one of the many benefits of Active Directory. Delegation of Active Directory objects enables the administrator to distribute administrative tasks among several assistant administrators without giving each assistant administrative privileges to the entire network.

# STUDY GUIDE

This section contains exercises that are designed to solidify your knowledge about implementing an OU structure and managing Active Directory objects, and to help you prepare for the Directory Services exam:

- **Assessment questions:** These questions test your knowledge of the Directory Service topics covered in this chapter. You'll find the answers to these questions at the end of this chapter.
- **Lab Exercises:** These exercises are hands-on practice activities that you perform on a computer. The lab in this chapter gives you an opportunity to practice implementing OUs and managing Active Directory objects.

## Assessment Questions

1. You want to create an organizational unit (OU) on a Windows 2000 Server computer that is a domain controller. Which tool should you use?
   A. Windows Explorer
   B. Active Directory Sites and Services
   C. Active Directory Domains and Trusts
   D. Active Directory Users and Computers
2. You want to use a Windows 2000 Professional computer on your Windows 2000 network to create an organizational unit (OU). How can you accomplish this?
   A. Install Active Directory on the Windows 2000 Professional computer. Then use Active Directory Domains and Trusts to create the OU.
   B. Install the ADMINPAK on the Windows 2000 Professional computer. Then use Active Directory Users and Computers to create the OU.

C. Install Active Directory on the Windows 2000 Professional computer. Then use Active Directory Users and Computers to create the OU.

D. Install the ADMINPAK on the Windows 2000 Professional computer. Then use Active Directory Sites and Services to create the OU.

3. You want to search for a specific shared folder object in Active Directory. Which tool should you use?

   A. Search

   B. Windows Explorer

   C. Active Directory Sites and Services

   D. Active Directory Users and Computers

4. You recently moved a user, JoeB, from the New York OU to the Los Angeles OU. Which of the following statements about JoeB are correct? (Choose all that apply.)

   A. JoeB acquires the inheritable permissions from the Los Angeles OU.

   B. JoeB retains the inheritable permissions from the New York OU.

   C. JoeB loses all previously inherited permissions from the New York OU.

   D. All users and groups that were previously assigned explicit permissions to manage JoeB can still manage JoeB.

5. You want to move the Philadelphia OU from the `acme1.com` domain to the `acme2.com` domain. Which tool should you use?

   A. `MoveTree.exe`

   B. The `move` command-line utility

   C. Server Extensions Administrator

   D. Active Directory Domains and Trusts

6. Which of the following statements about controlling access to Active Directory objects is true?

   A. Controlling access to an object in Active Directory, such as a shared folder, is the same as controlling access to the object itself.

   B. If I have the Full Control permission to a shared Windows NT printer on my network, I also have the Full Control permission to the object that represents this shared printer in Active Directory.

C. When user and group permissions to an Active Directory object differ, the permissions are additive, and usually the *least* restrictive permission is the user's effective permission.

D. Inherited permissions always take precedence over explicit permissions.

7. When you set permissions on Active Directory objects, what can you specify? (Choose all that apply.)

A. The users and groups that are specifically permitted or denied access to the object and/or its properties

B. Whether the object's permissions will be applied to only the object itself, or to the object and to all of its child objects

C. Whether the object will inherit, or be blocked from inheriting, permissions from its parent object

D. The permissions that will control access to a specific property of the object

8. You want to delegate administration of an OU to a specific user. How can you accomplish this? (Choose two.)

A. Use the Delegation of Control Wizard to delegate administration of the OU.

B. Use the Active Directory Installation Wizard to delegate administration of the OU.

C. Use Active Directory Users and Computers to manually assign the appropriate permissions to the user for the OU.

D. Use Active Directory Domains and Trusts to manually assign each of the individual Active Directory permissions to the user for the OU.

## Lab Exercises

The following lab is designed to give you practical experience working OUs and Active Directory objects.

# Lab 8-1 Implementing OUs and Managing Active Directory Objects


► Directory Services

The purpose of this lab is to provide you with an opportunity to implement OUs and manage Active Directory objects. You'll use Active Directory Users and Computers to perform most of the tasks in this lab.

There are six parts to this lab:

- Part 1: Implementing an Organizational Unit (OU) Structure
- Part 2: Locating Objects in Active Directory
- Part 3: Publishing Resources in Active Directory
- Part 4: Moving Objects in Active Directory
- Part 5: Controlling Access to Active Directory Objects
- Part 6: Delegating Administration of Active Directory Objects

Begin this lab by booting your computer to Windows 2000 Server and logging on as Administrator.

## Part 1: Implementing an Organizational Unit (OU) Structure

In this part, you use Active Directory Users and Computers to create several OUs.

1. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
2. In the left pane of the Active Directory Users and Computers dialog box, highlight domain1.mcse. Select Action ➪ New ➪ Organizational Unit.
3. In the New Object - Organizational Unit dialog box, type **HQ Seattle** and click OK.
4. In the Active Directory Users and Computers dialog box, select Action ➪ New ➪ Organizational Unit.
5. In the New Object - Organizational Unit dialog box, type **Denver** and click OK.

6. In the right pane of the Active Directory Users and Computers dialog box, double-click HQ Seattle. Then select Action ➪ New ➪ Organizational Unit.
7. In the New Object - Organizational Unit dialog box, type **Accounting** and click OK.
8. In the Active Directory Users and Computers dialog box, select Action ➪ New ➪ Organizational Unit.
9. In the New Object - Organizational Unit dialog box, type **Marketing** and click OK.
10. In the left pane of the Active Directory Users and Computers dialog box, highlight Denver. Then select Action ➪ New ➪ Organizational Unit.
11. In the New Object - Organizational Unit dialog box, type **R & D** and click OK.
12. In the Active Directory Users and Computers dialog box, select Action ➪ New ➪ Organizational Unit.
13. In the New Object - Organizational Unit dialog box, type **Manufacturing** and click OK.
14. In the Active Directory Users and Computers dialog box, select Action ➪ New ➪ Organizational Unit.
15. In the New Object - Organizational Unit dialog box, type **Information Services** and click OK. Continue on to Part 2.

### Part 2: Locating Objects in Active Directory

In this part, you use Active Directory Users and Computers to search for objects in Active Directory.

1. In the left pane of the Active Directory Users and Computers dialog box, highlight domain1.mcse. Select Action ➪ Find.
2. The Find Users, Contacts, and Groups dialog box appears. In the Name text box, type **administrator** and click Find Now.
3. Active Directory Users and Computers displays a group named Administrators and a user named Administrator in the bottom of the dialog box. Double-click the user named Administrator.
4. The Administrator Properties dialog box appears. Notice the numerous tabs in this Properties dialog box. On the General tab, fill in all of your personal information and click OK.

5. The Find Users, Contacts, and Groups dialog box reappears. In the Find drop-down list box, select Computers.
6. When the "Find in the Directory" dialog box is displayed, click OK.
7. In the "Computer name" text box, type **Server01** and click Find Now.
8. Active Directory Users and Computers displays a computer named SERVER01. Double-click SERVER01.
9. The SERVER01 Properties dialog box appears. Notice the various tabs. Type in a description of your computer on the General tab, and click OK.
10. Close the Find Computers dialog box. Close the Active Directory Users and Computers dialog box.

### Part 3: Publishing Resources in Active Directory

In this part you share a folder, and then publish the shared folder in Active Directory.

1. From the desktop, select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.
2. In the left pane, click the + next to My Computer. Click the + next to Local Disk (C:). Click the + next to Program Files. Right-click Accessories, and select Sharing from the menu that appears.
3. In the Accessories Properties dialog box, select the "Share this folder" option. Accept the default share name of Accessories. Click OK.
4. Close Windows Explorer.
5. Start Active Directory Users and Computers. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.)
6. In the left pane of the Active Directory Users and Computers dialog box, click the + next to domain1.mcse. Click the + next to Denver. Highlight Information Services. Select Action ➪ New ➪ Shared Folder.
7. In the New Object – Shared Folder dialog box, type **Accessories** in the Name text box. Then type **\\server01\accessories** in the "Network path" text box. Click OK.
8. The new shared folder object appears in the right pane of the Active Directory Users and Computers dialog box. You've now shared a folder and published it in Active Directory. Continue on to Part 4.

## Part 4: Moving Objects in Active Directory

In this part, you move the Information Services OU (and all of its contents) from the Denver OU into the HQ Seattle OU.

1. In the left pane of the Active Directory Users and Computers dialog box, highlight Information Services. Select Action ➪ Move.
2. In the Move dialog box, highlight HQ Seattle, and click OK.
3. In the left pane of the Active Directory Users and Computers dialog box, click the + next to HQ Seattle. Notice that the Information Services OU is now contained in the HQ Seattle OU. Highlight the Information Services OU. Notice that the shared folder named Accessories was also moved when the OU that contained it (Information Services) was moved. Continue on to Part 5.

## Part 5: Controlling Access to Active Directory Objects

In this part, you assign permissions to a group for a specific OU.

1. In the left pane of the Active Directory Users and Computers dialog box, select View ➪ Advanced Features.
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to HQ Seattle. Highlight Information Services. Select Action ➪ Properties.
3. In the Information Services Properties dialog box, click the Security tab.
4. On the Security tab, highlight the Account Operators group in the Name box. Then select the check boxes under "Allow" next to Read, Create All Child Objects, and Delete All Child Objects. Click Advanced.
5. In the Access Control Settings for Information Services dialog box, ensure that Account Operators is highlighted in the Permission Entries box. Click View/Edit.
6. In the Permission Entry for Information Services dialog box, select "This object and all child objects" from the "Apply onto" drop-down list box. Click OK.
7. In the Access Control Settings for Information Services dialog box, click OK.
8. In the Information Services Properties dialog box, click OK. Continue on to Part 6.

### Part 6: Delegating Administration of Active Directory Objects

In this part, you delegate authority to administer the Denver OU and all of its contents.

1. In the left pane of the Active Directory Users and Computers dialog box, highlight Denver. Select Action ➪ Delegate Control.
2. The Delegation of Control Wizard starts. Click Next.
3. In the Users or Groups screen, click Add.
4. In the Select Users, Computers, or Groups dialog box, double-click Server Operators. Click OK.
5. In the Users or Groups screen, click Next.
6. In the Tasks to Delegate screen, select the "Create a custom task to delegate" option and click Next.
7. The Active Directory Object Type screen appears. Accept the default setting to delegate control of "This folder, existing objects in this folder, and creation of new objects in this folder." Click Next.
8. In the Permissions screen, select the check box next to Full Control in the Permissions box. Click Next.
9. In the Completing the Delegation of Control Wizard screen, click Finish.

# Answers to Chapter Questions

## Chapter Pre-Test

1. An organizational unit (OU) is a type of Active Directory object. OUs are specifically designed to contain objects and other organizational units from their own domain. The purpose of OUs is to make network administration simpler.
2. Any two tasks in the following list are correct. You can use Active Directory Users and Computers to: create OUs; add users, groups, computers, contacts, printers, and shared folders to Active Directory; delete any object in Active Directory; configure the properties of any object in Active Directory; locate objects in Active Directory; publish resources in Active Directory; move objects in Active Directory; control access to and configure security for Active Directory objects; delegate administrative control of Active Directory objects.

3. The act of creating an Active Directory object for a shared folder, shared printer, or other network resource is called *publishing*.
4. A parent object is a container object that contains other objects. An object that is contained in the parent object is referred to as a child object.
5. The OU is the smallest container object in Active Directory to which you can delegate administrative authority.

## Assessment Questions

1. **D.** You can use Active Directory Users and Computers to create and manage OUs.
2. **B.** To use a Windows 2000 Professional computer to create an OU, you should first install the ADMINPAK on the Windows 2000 Professional computer, and then use Active Directory Users and Computers to create the OU. You can't install Active Directory on a Windows 2000 Professional computer.
3. **D.** To search for a specific shared folder in Active Directory, use Active Directory Users and Computers. You can use Windows Explorer to *browse* Active Directory, but you can't use it to search for a specific shared folder.
4. **A, C, D.** B is not correct because Joe loses all of his previously inherited permissions from the New York OU.
5. **A.** Use `MoveTree.exe` to move Active Directory objects from one domain to another.
6. **C.** Typically, when user and group permissions to an Active Directory object differ, the permissions are additive, and the *least* restrictive permission is the user's effective permission. There are, however, exceptions to this rule. All of the other statements are false.
7. **A, B, C, D.** All of the statements are true.
8. **A, C.** There are two ways to delegate administration of Active Directory objects: by using the Delegation of Control Wizard (found in Active Directory Users and Computers) and by using Active Directory Users and Computers to manually assign the appropriate permissions to the user for the OU.